

National Cyber Alert System

Cyber Security Bulletin SB09-271

[Archive](#)

Vulnerability Summary for the Week of September 21, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSA) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
php -- pro-bid	SQL injection vulnerability in auction_details.php in PHP Pro Bid allows remote attackers to execute arbitrary SQL commands via the auction_id parameter.	2009-09-24	7.5	CVE-2009-3336 VUPEN BID MILWoRM
alibasta -- com_koesubmit	PHP remote file inclusion vulnerability in koesubmit.php in the koeSubmit (com_koesubmit) component 1.0 for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	2009-09-23	7.5	CVE-2009-3333 BID MILWoRM
alphaplugin -- com_alphapoints	SQL injection vulnerability in frontend/assets/ajax/checkusername.php in the AlphaUserPoints (com_alphapoints) component 1.5.2 for Joomla! allows remote attackers to execute arbitrary SQL commands via the username2points parameter.	2009-09-24	7.5	CVE-2009-3342 VUPEN BID MILWoRM
andres_g_aragoneses -- prodler	PHP remote file inclusion vulnerability in include/prodler.class.php in ProdLer 2.0 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the sPath parameter.	2009-09-23	7.5	CVE-2009-3324 MILWoRM
andrew_sterling_hanenkamp -- rest_api_module	Multiple unspecified vulnerabilities in the Rest API module for Drupal have unknown impact and attack	2009-09-24	10.0	CVE-2009-3354 BID

rest_api_module	vectors.	24		BID CONFIRM
apple -- iphone_os	iPhone Mail in Apple iPhone OS, and iPhone OS for iPod touch, does not validate X.509 certificates, which allows man-in-the-middle attackers to spoof arbitrary SSL e-mail servers via a crafted certificate.	2009-09-21	7.5	CVE-2009-3273 XF BID BUGTRAQ
apple -- itunes	Buffer overflow in Apple iTunes before 9.0.1 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted .pls file.	2009-09-24	9.3	CVE-2009-2817 BID CONFIRM APPLE
breedveld -- com_album	Directory traversal vulnerability in the Roland Breedveld Album (com_album) component 1.14 for Joomla! allows remote attackers to access arbitrary directories and have unspecified other impact via a .. (dot dot) in the target parameter to index.php.	2009-09-23	7.5	CVE-2009-3318 BID MILWoRM
cfshopkart -- cf_shopkart	SQL injection vulnerability in index.cfm in CF ShopKart 5.4 beta allows remote attackers to execute arbitrary SQL commands via the itemid parameter in a ViewDetails action, a different vector than CVE-2008-6320.	2009-09-23	7.5	CVE-2009-3309 XF BID MILWoRM
cmscontrol -- cmscontrol	SQL injection vulnerability in index.php in CMScontrol Content Management System 7.x allows remote attackers to execute arbitrary SQL commands via the id_menu parameter.	2009-09-23	7.5	CVE-2009-3326 MILWoRM
craig_barratt -- backuppc	CgiUserConfigEdit in BackupPC 3.1.0, when SSH keys and Rsync are in use in a multi-user environment, does not restrict users from the ClientNameAlias function, which allows remote authenticated users to read and write sensitive files by modifying ClientNameAlias to match another system, then initiating a backup or restore.	2009-09-24	8.5	CVE-2009-3369 SECUNIA OSVDB MISC
d-link -- dir-400	Buffer overflow on the D-Link DIR-400 wireless router allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.10 through 8.11. NOTE: as of 20090917, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-24	10.0	CVE-2009-3347 SECTRACK BID OSVDB SECUNIA MISC
datavore -- gyro	SQL injection vulnerability in Datavore Gyro 5.0 allows remote attackers to execute arbitrary SQL commands via the cid parameter in a cat action to the home component.	2009-09-24	7.5	CVE-2009-3349 XF MILWoRM
ddlcms -- ddl_cms	Multiple PHP remote file inclusion vulnerabilities in DDL CMS 1.0 allow remote attackers to execute arbitrary PHP code via a URL in the wwwRoot parameter to (1) header.php, (2) submit.php, (3) submitted.php, and (4) autosubmitter/index.php.	2009-09-23	7.5	CVE-2009-3331 XF MILWoRM
dimofinf -- dawaween	SQL injection vulnerability in poems.php in DCI-Designs Dawaween 1.03 allows remote attackers to execute arbitrary SQL commands via the id parameter in a sec list action, a different vector than CVE-2006-1018.	2009-09-23	7.5	CVE-2009-3319 BID BUGTRAQ

effectmatrix -- magic_morph	Stack-based buffer overflow in EffectMatrix (E.M.) Magic Morph 1.95b allows remote attackers to execute arbitrary code via a long string in a .mor file.	2009-09-24	9.3	CVE-2009-3338 VUPEN MILWoRM SECUNIA
eliteladders -- elite_gaming_ladders	SQL injection vulnerability in ladders.php in Elite Gaming Ladders 3.2 allows remote attackers to execute arbitrary SQL commands via the platform parameter.	2009-09-23	7.5	CVE-2009-3314 XF VUPEN MILWoRM SECUNIA OSVDB
exeter -- winplot	Stack-based buffer overflow in Winplot 1.25.0.1 allows user-assisted remote attackers to execute arbitrary code via a crafted Plot2D (.wp2) file.	2009-09-23	9.3	CVE-2009-3329 MILWoRM SECUNIA
fanupdate -- fanupdate	SQL injection vulnerability in show-cat.php in FanUpdate 2.2.1 allows remote attackers to execute arbitrary SQL commands via the listingid parameter.	2009-09-23	7.5	CVE-2009-3308 VUPEN MILWoRM SECUNIA
focusdev -- com_surveymanager	SQL injection vulnerability in the Focusplus Developments Survey Manager (com_surveymanager) component 1.5.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the stype parameter in an editsurvey action to index.php.	2009-09-23	7.5	CVE-2009-3325 VUPEN BID MILWoRM
frank_lichtenheld -- fsphp	Multiple PHP remote file inclusion vulnerabilities in FSphp 0.2.1 allow remote attackers to execute arbitrary PHP code via a URL in the FSPHP_LIB parameter to (1) FSphp.php, (2) navigation.php, and (3) pathwrite.php in lib/.	2009-09-23	7.5	CVE-2009-3307 VUPEN MILWoRM
ftpshe ll -- ftpshell	Stack-based buffer overflow in FTPShell Client 4.1 RC2 allows remote FTP servers to execute arbitrary code via a long response to a PASV command.	2009-09-24	9.3	CVE-2009-3364 XF VUPEN BID OSVDB MILWoRM SECUNIA
go-oo -- go-oo	Multiple heap-based buffer overflows in cppcanvas/source/mtfrenderer/emfplus.cxx in Go-oo 2.x and 3.x before 3.0.1, previously named ooo-build and related to OpenOffice.org (OOo), allow remote attackers to execute arbitrary code via a crafted EMF+ file, a similar issue to CVE-2008-2238.	2009-09-21	9.3	CVE-2009-2140 CONFIRM
hotwebscripts -- hotweb_rentals	SQL injection vulnerability in details.asp in HotWeb Rentals allows remote attackers to execute arbitrary SQL commands via the PropId parameter.	2009-09-24	7.5	CVE-2009-3343 MILWoRM
hp -- storageworks_1/8_g2_tape_autoloader hp -- storageworks_msl2024_tape_library hp -- storageworks_msl4048_tape_library hp --	Unspecified vulnerability in the Remote Management Interface (RMI) for MSL Tape Libraries and 1/8 G2 Tape Autoloaders in HP StorageWorks 1/8 G2 Tape Autoloader firmware 2.30 and earlier, MSL2024 Tape Library firmware 4.20 and earlier, MSL4048 Tape Library firmware 6.50 and earlier, and MSL8096 Tape Library firmware	2009-09-24	8.5	CVE-2009-2680 HP HP

hp -- storageworks_msl8096_tape_library	8.90 and earlier allows remote attackers to cause a denial of service via unknown vectors.			
hp -- hp-ux	Unspecified vulnerability in Role-Based Access Control (RBAC) in HP HP-UX B.11.23 and B.11.31 allows local users to bypass intended access restrictions via unknown vectors.	2009-09-24	7.2	CVE-2009-2682 BID HP HP
ibm -- websphere_application_server	Unspecified vulnerability in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.27 allows remote attackers to cause a denial of service via unknown vectors, related to "an error in fixpacks 6.1.0.23 and 6.1.0.25."	2009-09-21	7.8	CVE-2009-2744 MISC
jforjoomla -- com_jreservation	SQL injection vulnerability in the JReservation (com_jreservation) component 1.0 and 1.5 for Joomla! allows remote attackers to execute arbitrary SQL commands via the pid parameter in a propertypanel action to index.php.	2009-09-23	7.5	CVE-2009-3316 XF BID MILWoRM SECUNIA OSVDB
joomlahbs -- com_hbssearch	Multiple SQL injection vulnerabilities in the Hotel Booking Reservation System (aka HBS or com_hbssearch) component for Joomla! allow remote attackers to execute arbitrary SQL commands via the (1) h_id, (2) id, and (3) rid parameters to longDesc.php, and the h_id parameter to (4) detail.php, (5) detail1.php, (6) detail2.php, (7) detail3.php, (8) detail4.php, (9) detail5.php, (10) detail6.php, (11) detail7.php, and (12) detail8.php, different vectors than CVE-2008-5865, CVE-2008-5874, and CVE-2008-5875.	2009-09-24	7.5	CVE-2009-3357 BID BUGTRAQ MILWoRM SECUNIA MISC
kristy_frey -- node_browser_module	Multiple unspecified vulnerabilities in the Node Browser module for Drupal have unknown impact and attack vectors.	2009-09-24	10.0	CVE-2009-3351 BID CONFIRM
lhacky -- com_jinc	SQL injection vulnerability in the Lhacky! Extensions Cave Joomla! Integrated Newsletters Component (aka JINC or com_jinc) component 0.2 for Joomla! allows remote attackers to execute arbitrary SQL commands via the newsid parameter in a messages action to index.php.	2009-09-23	7.5	CVE-2009-3334 BID MILWoRM
linksys -- wrt54gl	Buffer overflow on the Linksys WRT54GL wireless router allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.10 through 8.11. NOTE: as of 20090917, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-24	10.0	CVE-2009-3341 SECTRACK SECUNIA MISC
linux -- kernel linux -- linux_kernel	Integer signedness error in the find_ie function in net/wireless/scan.c in the cfg80211 subsystem in the Linux kernel before 2.6.31.1-rc1 allows remote attackers to cause a denial of service (soft lockup) via malformed packets.	2009-09-21	7.8	CVE-2009-3280 CONFIRM CONFIRM
	The kvm_emulate_hypercall function in arch/x86/kvm/x86.c in KVM in the Linux kernel 2.6.25-rc1, and other versions before 2.6.31, when			CVE-2009-

linux -- linux_kernel	running on x86 systems, does not prevent access to MMU hypercalls from ring 0, which allows local guest OS users to cause a denial of service (guest kernel crash) and read or write guest kernel memory via unspecified "random addresses."	2009-09-22	7.2	CVE-2009-3290 CONFIRM
livestreet -- livestreet	update/update_0.1.2_to_0.2.php in LiveStreet 0.2 does not require administrative authentication, which allows remote attackers to perform DROP TABLE operations via unspecified vectors.	2009-09-18	7.5	CVE-2009-3261 MISC
macournoyer -- thin	lib/thin/connection.rb in Thin web server before 1.2.4 relies on the X-Forwarded-For header to determine the IP address of the client, which allows remote attackers to spoof the IP address and hide activities via a modified X-Forwarded-For header.	2009-09-22	7.5	CVE-2009-3287 CONFIRM
mcafee -- email_and_web_security_appliance	Unspecified vulnerability in McAfee Email and Web Security Appliance 5.1 VMtrial allows remote attackers to read arbitrary files via unknown vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.9 through 8.11. NOTE: as of 20090917, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-24	7.8	CVE-2009-3339 SECTRACK SECUNIA MISC
nelogic -- nephp_publisher	SQL injection vulnerability in admin/index.php in NeLogic Nephph Publisher Enterprise 3.5.9 and 4.5 allows remote attackers to execute arbitrary SQL commands via the Username field.	2009-09-23	7.5	CVE-2009-3315 XF BID MILWoRM
paul_gibbs -- php-ipnmonitor	SQL injection vulnerability in index.php in PHP-IPNMonitor allows remote attackers to execute arbitrary SQL commands via the maincat_id parameter.	2009-09-24	7.5	CVE-2009-3361 MILWoRM
php -- php	The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.	2009-09-22	7.5	CVE-2009-3291 CONFIRM CONFIRM
php -- php	Unspecified vulnerability in PHP before 5.2.11 has unknown impact and attack vectors related to "missing sanity checks around exif processing."	2009-09-22	7.5	CVE-2009-3292 CONFIRM CONFIRM OSVDB SECUNIA
php -- php	Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."	2009-09-22	7.5	CVE-2009-3293 CONFIRM
plohni -- image_voting	SQL injection vulnerability in index.php in Image voting 1.0 allows remote attackers to execute arbitrary SQL commands via the show parameter.	2009-09-24	7.5	CVE-2009-3356 XF MILWoRM SECUNIA
richrumble -- clearsite	PHP remote file inclusion vulnerability in include/header.php in ClearSite 4.50 allows remote attackers to execute arbitrary PHP code via a URL in the cs_base_path parameter.	2009-09-23	7.5	CVE-2009-3306 VUPEN MILWoRM

robig -- barosmini	Multiple PHP remote file inclusion vulnerabilities in Banner ROTation System mini (BAROSmini) 0.32.595 allow remote attackers to execute arbitrary PHP code via a URL in the baros_path parameter to (1) include/common_functions.php, and the main_path parameter to (2) lib_users.php, (3) lib_stats.php, and (4) lib_slots.php in include/lib/.	2009-09-23	7.5	CVE-2009-3323 XF MILWoRM
roshan_shah -- subdomain_manager	Multiple unspecified vulnerabilities in the Subdomain Manager module for Drupal have unknown impact and attack vectors.	2009-09-24	10.0	CVE-2009-3350 BID CONFIRM
roshan_shah -- quota_by_role	Multiple unspecified vulnerabilities in the quota_by_role (Quota by role) module for Drupal have unknown impact and attack vectors.	2009-09-24	10.0	CVE-2009-3352 BID CONFIRM
s9y -- serendipity_freetag-plugin	SQL injection vulnerability in the Freetag (serendipity_event_freetag) plugin before 3.09 for Serendipity (S9Y) allows remote attackers to execute arbitrary SQL commands via an unspecified parameter associated with Meta keywords in a blog entry.	2009-09-24	7.5	CVE-2009-3337 BID SECUNIA CONFIRM
sap -- crystal_reports_server	Heap-based buffer overflow in SAP Crystal Reports Server 2008 has unknown impact and attack vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.3 through 8.11. NOTE: as of 20090917, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-24	10.0	CVE-2009-3345 BID SECUNIA MISC
sap -- crystal_reports_server	Unspecified vulnerability in SAP Crystal Reports Server 2008 allows remote attackers to execute arbitrary code via unknown vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.3 through 8.11. NOTE: as of 20090917, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-24	10.0	CVE-2009-3346 BID SECUNIA MISC
shalwan -- zainu	SQL injection vulnerability in index.php in Zainu 1.0 allows remote attackers to execute arbitrary SQL commands via the album_id parameter in an AlbumSongs action.	2009-09-23	7.5	CVE-2009-3310 XF VUPEN BID MILWoRM SECUNIA
siemens -- gigaset_se361_wlan_router	The Siemens Gigaset SE361 WLAN router allows remote attackers to cause a denial of service (device reboot) via a flood of crafted TCP packets to port 1723.	2009-09-23	7.8	CVE-2009-3322 BID BUGTRAQ OSVDB MILWoRM SECUNIA
sopinet -- com_jbudgetsmagic	SQL injection vulnerability in the JBudgetsMagic (com_jbudgetsmagic) component 0.3.2 through 0.4.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the bid parameter in a	2009-09-23	7.5	CVE-2009-3332 BID 3332 BID MILWoRM

	mybudget action to index.php.			MILWoRM
steve_lockwood -- node2node	Multiple unspecified vulnerabilities in the Node2Node module for Drupal have unknown impact and attack vectors.	2009-09-24	10.0	CVE-2009-3353 BID CONFIRM
sun -- opensolaris	Multiple unspecified vulnerabilities in the (1) iscsiadm and (2) iscsitadm programs in Sun Solaris 10, and OpenSolaris snv_28 through snv_109, allow local users with certain RBAC execution profiles to gain privileges via unknown vectors related to the libima library.	2009-09-24	7.2	CVE-2009-3390 SUNALERT CONFIRM
sznews -- sznews	PHP remote file inclusion vulnerability in printnews.php3 in SZNews 2.7 allows remote attackers to execute arbitrary PHP code via a URL in the id parameter.	2009-09-24	7.5	CVE-2009-3362 SECUNIA MISC OSVDB
thecodeweasel -- opensiteadmin	PHP remote file inclusion vulnerability in pages/pageHeader.php in OpenSiteAdmin 0.9.7 BETA allows remote attackers to execute arbitrary PHP code via a URL in the path parameter, a different vector than CVE-2008-0648.	2009-09-23	7.5	CVE-2009-3317 XF BID MILWoRM
thomas_cuchta -- rash	Multiple SQL injection vulnerabilities in RASH Quote Management System (RQMS) 1.2.2 allow remote attackers to execute arbitrary SQL commands via (1) the search parameter in a search action, (2) the quote parameter in a quote addition, or (3) a User_Name cookie in unspecified administrative actions. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-09-18	7.5	CVE-2009-3259 XF SECUNIA OSVDB OSVDB OSVDB
tourismscripts -- adult_portal_escort_listing	SQL injection vulnerability in profile.php in Tourism Scripts Adult Portal escort listing allows remote attackers to execute arbitrary SQL commands via the user_id parameter.	2009-09-24	7.5	CVE-2009-3358 XF MILWoRM
traza -- aurora	PHP remote file inclusion vulnerability in addons/modules/sysmanager/plugins/install.plugin.php in Aurora CMS 1.0.2 allows remote attackers to execute arbitrary PHP code via a URL in the AURORA_MODULES_FOLDER parameter.	2009-09-24	7.5	CVE-2009-3365 MILWoRM
turtus -- turtushout	SQL injection vulnerability in the TurtuShout component 0.11 for Joomla! allows remote attackers to execute arbitrary SQL commands via the Name field.	2009-09-24	7.5	CVE-2009-3335 XF MILWoRM
ultimatevideosite -- ultimate_player	Multiple stack-based buffer overflows in Ultimate Player 1.56 beta allow remote attackers to execute arbitrary code via a long string in a (1) .m3u or (2) .upl playlist file.	2009-09-18	9.3	CVE-2009-3254 VUPEN MILWoRM
	Multiple directory traversal vulnerabilities in vtiger CRM 5.0.4 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in (1) the module parameter to graph.php; or the (2) module or (3) file parameter to include/Ajax/CommonAjax.php, reachable through modules/Campaigns/CampaignsAjax.php, modules/SalesOrder/SalesOrderAjax.php, modules/System/SystemAjax.php,			

vtiger -- vtiger_crm	modules/Products/ProductsAjax.php, modules/uploads/uploadsAjax.php, modules/Dashboard/DashboardAjax.php, modules/Potentials/PotentialsAjax.php, modules/Notes/NotesAjax.php, modules/Faq/FaqAjax.php, modules/Quotes/QuotesAjax.php, modules/Utilities/UtilitiesAjax.php, modules/Calendar/ActivityAjax.php, modules/Calendar/CalendarAjax.php, modules/PurchaseOrder/PurchaseOrderAjax.php, modules/HelpDesk/HelpDeskAjax.php, modules/Invoice/InvoiceAjax.php, modules/Accounts/AccountsAjax.php, modules/Reports/ReportsAjax.php, modules/Contacts/ContactsAjax.php, and modules/Portal/PortalAjax.php; and allow remote authenticated users to include and execute arbitrary local files via a .. (dot dot) in the step parameter in an Import action to the (4) Accounts, (5) Contacts, (6) HelpDesk, (7) Leads, (8) Potentials, (9) Products, or (10) Vendors module, reachable through index.php and related to modules/Import/index.php and multiple Import.php files.	2009-09-18	7.5	CVE-2009-3249 VUPEN MISC MISC BID OSVDB MILWoRM SECUNIA BUGTRAQ
webilix -- wx-guestbook	Multiple SQL injection vulnerabilities in WX-Guestbook 1.1.208 allow remote attackers to execute arbitrary SQL commands via the (1) QUERY parameter to search.php and (2) USERNAME parameter to login.php. NOTE: some of these details are obtained from third party information.	2009-09-23	7.5	CVE-2009-3327 MILWoRM SECUNIA

[Back to top](#)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	C S
apple -- safari apple -- iphone_os	Apple Safari on iPhone OS 3.0.1 allows remote attackers to cause a denial of service (application crash) via a long tel: URL in the SRC attribute of an IFRAME element.	2009-09-21	
apple -- safari	Stack consumption vulnerability in WebKit.dll in WebKit in Apple Safari 3.2.3, and possibly other versions before 4.1.2, allows remote attackers to cause a denial of service (application crash) via JavaScript code that calls eval on a long string composed of A/ sequences.	2009-09-21	
cpecreator -- cp_creator	SQL injection vulnerability in index.php in cP Creator 2.7.1, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the tickets parameter in a support ticket action.	2009-09-23	
datavore -- gyro	Cross-site scripting (XSS) vulnerability in Datavore Gyro 5.0 allows remote attackers to inject arbitrary web script or HTML via the cid parameter in a cat action to the home component.	2009-09-24	
	Multiple cross-site scripting (XSS) vulnerabilities in Datemill 1.0 allow remote	2009-09-24	

datemill -- datemill	attackers to inject arbitrary web script or HTML via the (1) return parameter to photo_view.php, and st parameter to (2) photo_search.php and (3) search.php.	2009-09-24	
datetopia -- buy_dating_site	Cross-site scripting (XSS) vulnerability in profile.php in Datetopia Buy Dating Site 1.0 allows remote attackers to inject arbitrary web script or HTML via the s_r parameter.	2009-09-24	
datetopia -- match_agency_biz	Multiple cross-site scripting (XSS) vulnerabilities in Match Agency BiZ 1.0 allow remote attackers to inject arbitrary web script or HTML via the (1) important parameter to edit_profile.php and (2) pid parameter to report.php.	2009-09-24	
fmyclone -- fmyclone	Multiple SQL injection vulnerabilities in FMyClone 2.3 allow remote attackers to execute arbitrary SQL commands via the comp parameter to (1) index.php and (2) editComments.php, and (3) allow remote authenticated administrators to execute arbitrary SQL commands via the id parameter in a comment action to edit.php.	2009-09-23	
freesshd -- freesshd	Unspecified vulnerability in FreeSSHD 1.2.4 allows remote attackers to cause a denial of service via unknown vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.11. NOTE: as of 20090917, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-24	
gnome -- glib	The g_file_copy function in glib 2.0 sets the permissions of a target file to the permissions of a symbolic link (777), which allows user-assisted local users to modify files of other users, as demonstrated by using Nautilus to modify the permissions of the user home directory.	2009-09-22	
google -- chrome	Google Chrome 0.2.149.29 and earlier allows remote attackers to cause a denial of service (unusable browser) by calling the window.print function in a loop, aka a "printing DoS attack," possibly a related issue to CVE-2009-0821.	2009-09-18	
google -- chrome	Cross-site scripting (XSS) vulnerability in Google Chrome 2.x and 3.x before 3.0.195.21 allows remote attackers to inject arbitrary web script or HTML via a (1) RSS or (2) Atom feed, related to the rendering of the application/rss+xml content type as XML "active content."	2009-09-18	
google -- chrome	The getSVGDocument method in Google Chrome before 3.0.195.21 omits an unspecified "access check," which allows remote web servers to bypass the Same Origin Policy and conduct cross-site scripting attacks via unknown vectors, related to a user's visit to a different web server that hosts an SVG document.	2009-09-18	
	Google Chrome 1.0.154.48 and earlier allows remote attackers to cause a denial	2009-09-18	

google -- chrome	of service (CPU consumption) via an automatically submitted form containing a KEYGEN element, a related issue to CVE-2009-1828.	2009-09-18
ibm -- websphere_application_server	Cross-site scripting (XSS) vulnerability in Eclipse Help in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.27 allows remote attackers to inject arbitrary web script or HTML via unspecified input.	2009-09-21
joomlahbs -- com_hbssearch	Cross-site scripting (XSS) vulnerability in the Hotel Booking Reservation System (aka HBS or com_hbssearch) component for Joomla! allows remote attackers to inject arbitrary web script or HTML via the adult parameter in a showhoteldetails action to index.php.	2009-09-24
kernel -- linux_kernel linux -- linux_kernel	The sg_build_indirect function in drivers/scsi/sg.c in Linux kernel 2.6.28-rc1 through 2.6.31-rc8 uses an incorrect variable when accessing an array, which allows local users to cause a denial of service (kernel OOPS and NULL pointer dereference), as demonstrated by using xcdroast to duplicate a CD. NOTE: this is only exploitable by users who can open the cdrom device.	2009-09-22
linux -- kernel	The z9ocrypt_unlocked_ioctl function in the z9ocrypt driver in the Linux kernel 2.6.9 does not perform a capability check for the Z90QUIESCE operation, which allows local users to leverage euid 0 privileges to force a driver outage.	2009-09-18
linux -- linux_kernel	NFSv4 in the Linux kernel 2.6.18, and possibly other versions, does not properly clean up an inode when an O_EXCL create fails, which causes files to be created with insecure settings such as setuid bits, and possibly allows local users to gain privileges, related to the execution of the do_open_permission function even when a create fails.	2009-09-22
microsoft -- ie	Microsoft Internet Explorer 7 through 7.0.6000.16711 allows remote attackers to cause a denial of service (unusable browser) by calling the window.print function in a loop, aka a "printing DoS attack," possibly a related issue to CVE-2009-0821.	2009-09-18
microsoft -- enterprise_library	Blocks/Common/Src/Configuration/Manageability/Adm/AdmContentBuilder.cs in Microsoft patterns & practices Enterprise Library (aka EntLib) allows context-dependent attackers to cause a denial of service (CPU consumption) via an input string composed of many \ (backslash) characters followed by a " (double quote), related to a certain regular expression, aka a "ReDoS" vulnerability.	2009-09-21
mozilla -- firefox	Mozilla Firefox 3.0.1 and earlier allows remote attackers to cause a denial of service (browser hang) by calling the window.print function in a loop, aka a "printing DoS attack," possibly a related issue to CVE-2009-0821.	2009-09-18
mozilla -- firefox	Mozilla Firefox 3.6a1, 3.5.2, and earlier 2.x and 3.x versions on Linux uses a predictable /tmp pathname for files selected from the Downloads window, which allows local users to replace an arbitrary downloaded file by placing a file in a /tmp location before the download occurs, possibly related to the Archive Manager component. NOTE: some of these details are obtained from third party information.	2009-09-21
nasd -- corenet1	Zoran/WinFormsAdvansed/RegeularDataToXML/Form1.cs in WinFormsAdvansed in NASD CORE.NET Terelik (aka corenet1) allows context-dependent attackers to cause a denial of service (CPU consumption) via an input string composed of many alphabetic characters followed by a ! (exclamation point), related to a certain regular expression, aka a "ReDoS" vulnerability.	2009-09-21
	The kernel in NetBSD, probably 5.0.1 and earlier, on x86 platforms does not	

netbsd -- netbsd	properly handle a pre-commit failure of the iret instruction, which might allow local users to gain privileges via vectors related to a tempEIP pseudocode variable that is outside of the code-segment limits.	2009-09-18
opera -- opera	Cross-site scripting (XSS) vulnerability in Opera 9 and 10 allows remote attackers to inject arbitrary web script or HTML via a (1) RSS or (2) Atom feed, related to the rendering of the application/rss+xml content type as "scripted content." NOTE: the vendor reportedly considers this behavior a "design feature," not a vulnerability.	2009-09-18
opera -- opera	Unspecified vulnerability in Opera 9 and 10 allows remote attackers to conduct cross-site scripting (XSS) attacks and obtain "complete control over feeds" via a (1) RSS or (2) Atom feed, related to the rendering of the application/rss+xml content type as "scripted content."	2009-09-18
opera -- opera	Opera 9.52 and earlier allows remote attackers to cause a denial of service (CPU consumption) via a series of automatic submissions of a form containing a KEYGEN element, a related issue to CVE-2009-1828.	2009-09-18
php -- php	The popen API function in TSRM/tsrm_win32.c in PHP before 5.2.11, when running on certain Windows operating systems, allows context-dependent attackers to cause a denial of service (crash) via a crafted (1) "e" or (2) "er" string in the second argument (aka mode), possibly related to the _fdopen function in the Microsoft C runtime library. NOTE: this might not cross privilege boundaries except in rare cases in which the mode argument is accessible to an attacker outside of an application that uses the popen function.	2009-09-22
phpspot -- php_&_css_bbs phpspot -- php_bbs phpspot -- php_bbs_ce phpspot -- php_image_capture_bbs phpspot -- php_rss_builder phpspot -- webshot	Cross-site scripting (XSS) vulnerability in phpspot PHP BBS, PHP Image Capture BBS, PHP & CSS BBS, PHP BBS CE, PHP_RSS_Builder, and webshot, dated before 20090914, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to cookies.	2009-09-22
phpspot -- php_&_css_bbs phpspot -- php_bbs phpspot -- php_bbs_ce phpspot -- php_image_capture_bbs phpspot -- php_rss_builder phpspot -- webshot	Directory traversal vulnerability in phpspot PHP BBS, PHP Image Capture BBS, PHP & CSS BBS, PHP BBS CE, PHP_RSS_Builder, and webshot, dated before 20090914, allows remote attackers to read arbitrary files via unspecified vectors.	2009-09-22
plohni -- an_image_gallery	Directory traversal vulnerability in navigation.php in An image gallery 1.0 allows remote attackers to list arbitrary directories via a .. (dot dot) in the path parameter.	2009-09-24
plohni -- an_image_gallery	Multiple cross-site scripting (XSS) vulnerabilities in An image gallery 1.0 allow remote attackers to inject arbitrary web script or HTML via the path parameter to (1) index.php and (2) main.php, and the (3) show parameter to main.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-09-24
postfix -- postfix	The postfix.postinst script in the Debian GNU/Linux and Ubuntu postfix 2.5.5 package grants the postfix user write access to /var/spool/postfix/pid, which might allow local users to conduct symlink attacks that overwrite arbitrary files.	2009-09-21
qnap -- ts-239_pro_turbo_nas qnap -- ts-639_pro_turbo_nas	The QNAP TS-239 Pro and TS-639 Pro with firmware 2.1.7 0613, 3.1.0 0627, and 3.1.1 0815 create an undocumented recovery key and store it in the ENCK variable in flash memory, which allows local users to bypass the passphrase requirement and decrypt the hard drive by reading this variable, deobfuscating	2009-09-21

039_pro_turbo_nas	the key, and running a cryptsetup luksOpen command.		
qnap -- ts-239_pro_turbo_nas qnap -- ts-639_pro_turbo_nas	The QNAP TS-239 Pro and TS-639 Pro with firmware 2.1.7 0613, 3.1.0 0627, and 3.1.1 0815 use the rand library function to generate a certain recovery key, which makes it easier for local users to determine this key via a brute-force attack.	2009-09-21	
qnap -- ts-239_pro_turbo_nas qnap -- ts-639_pro_turbo_nas	The QNAP TS-239 Pro and TS-639 Pro with firmware 2.1.7 0613, 3.1.0 0627, and 3.1.1 0815 create a LUKS partition by using the AES-256 cipher in plain CBC mode, which allows local users to obtain sensitive information via a watermark attack.	2009-09-21	
rssmediascript -- rssmediascript	Cross-site scripting (XSS) vulnerability in index.php in RSSMediaScript allows remote attackers to inject arbitrary web script or HTML via the page parameter.	2009-09-23	
sap -- crystal_reports_server	Unspecified vulnerability in SAP Crystal Reports Server 2008 on Windows XP allows attackers to cause a denial of service (infinite loop) via unknown vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.3 through 8.11. NOTE: as of 20090917, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-09-24	
saphplession -- saphplession	SQL injection vulnerability in SaphpLesson 4.3, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the CLIENT_IP HTTP header.	2009-09-23	
tomex -- phppollscript	PHP remote file inclusion vulnerability in php/init.poll.php in phpPollScript 1.3 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a crafted URL in the include_class parameter.	2009-09-23	
ufku_bayburt -- bueditor	Cross-site scripting (XSS) vulnerability in the BUEditor module 5.x before 5.x-1.2 and 6.x before 6.x-1.4, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via input to the "plain textarea editor."	2009-09-24	
webilix -- wx-guestbook	Cross-site scripting (XSS) vulnerability in sign.php in WX-Guestbook 1.1.208 allows remote attackers to inject arbitrary web script or HTML via the sName parameter (aka the name field). NOTE: some of these details are obtained from third party information.	2009-09-23	
xenu_by -- datavault	DataVault.Tesla/Impl/TypeSystem/AssociationHelper.cs in datavault allows context-dependent attackers to cause a denial of service (CPU consumption) via an input string composed of an [(open bracket) followed by many commas, related to a certain regular expression, aka a "ReDoS" vulnerability.	2009-09-21	
zenas -- paolink	Cross-site scripting (XSS) vulnerability in scrivi.php in Zenas PaoLink (aka PaoLink) 1.0 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2009-09-23	

[Back to top](#)

Low Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- websphere_application_server	IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.27 does not properly handle an exception occurring after use of wsadmin scripts and configuration of JAAS-J2C Authentication Data, which allows local users to obtain sensitive information by reading the First Failure Data Capture (FFDC) log file.	2009-09-21	2.1	CVE-2009-2743 MISC
vtiger -- vtiger_crm	vtiger CRM before 5.1.0 allows remote authenticated users to bypass the permissions on the (1) Account Billing Address and (2) Shipping Address fields in a profile by creating a Sales Order (SO) associated with that profile.	2009-09-18	3.6	CVE-2009-3257 CONFIRM SECUNIA

[Back to top](#)

Last updated September 28, 2009

[Print This Document](#)